

Appln No. 09/690,796  
Amdt date July 18, 2008  
Reply to Office action of February 25, 2008

**REMARKS/ARGUMENTS**

Claims 1, 5-10, 17, 22, 42, 50-52, and 55-59 are currently pending. Claims 1 and 50 are amended.

Applicant thanks the Examiner for his time for the telephonic interviews conducted on July 2, and July 9, 2008.

**The Examiner still has not acknowledged the IDS that was filed September 13, 2006. Applicants respectfully request acknowledgment of the above-mentioned IDS by initialing and returning the attached copy of the same IDS.**

Claims 1, 6-10, 17, 22, 42, 50-52, and 55-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis et al. (US 6,233,565), in view of Iyengar (U.S. 5,961,601). Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis et al., and Iyengar, in view of Bosen et al. (U.S. 5,060,263). Applicant respectfully submits that all of the pending claims are patentable over the cited references.

Independent claim 1 includes, among other limitations, "a plurality of stateless cryptographic devices, each of the plurality of stateless cryptographic devices configured to perform authentication, processing value for the VBI, and generation of indicia data for the plurality of users, wherein before each of the authentication, processing value, and generation of indicia data for a given user is performed, an available cryptographic device in the server system retrieves the data record for the given user directly from the database and uses the private key to verify the retrieved data record." None of the cited references, alone or in combination, teach or suggest the above limitations.

First, regarding the limitation of "a plurality of stateless cryptographic devices," there is no teaching that the cryptographic "modules" of Lewis are stateless. Rather, in the system of Lewis "each client 2n has a cryptographic module 12n and the RSP server 4 has a cryptographic module 14. The server cryptographic module 14 serves three functions: (1) authentication, (2) encryption, and (3) authorization. Authentication is the only function that requires interaction with a client cryptographic module 12." (Col. 21, lines 12-17, underlining is added.). Therefore,

Lewis has one (central) server cryptographic module 14, and many client cryptographic modules 12, one for each client and dedicated to that client. Additionally, Lewis teaches that his cryptographic modules are stateless.

The Examiner refers to Iyengar's "stateless network protocols" as teaching "stateless cryptographic devices." Applicant respectfully disagrees. Iyengar is very clear about the definition of a stateless protocol. For example, Iyengar clarifies that "Many network protocols between a client and server are stateless. This means that every request from a client to a server is treated independently. The server has no record of previous connections. HTTP is an example of a stateless protocol. Two advantages of using stateless protocols are efficiency and simplicity." (Col. 3, line 66 to col. 4, line 4.). One skilled in the art would readily understand that a "stateless device" is different than a "stateless protocol," each having its unique characteristics, advantages, and challenges.

A "stateless protocol," as Iyengar defines a "server application which wishes to preserve state [for a stateless protocol] must provide a list of all URL's which might make use of the state." (Col. 9, lines 12-14.). However, a stateless cryptographic device means "a PSD package [a database record] can be passed to any device because the application does not rely upon any information about what occurred with the previous PSD package. Therefore, multiple cryptographic modules can also be added to each appropriate subsystem in order to handle increased loads." (Page 8, lines 24-28).

As a result, the combination of Lewis and Iyengar does not teach or suggest the above limitation.

**Second**, regarding the newly added limitation of "each of the plurality of stateless cryptographic devices . . . uses the private key to verify the retrieved data record," none of the cited references teach or suggest the above limitation.

Lewis teaches that the "main function of the client cryptographic module 12 is to protect the [respective]customer's private key from both intrusion and corruption. The customer's private key is used to authenticate the client 2 to the server 4." (Col. 22, lines 6-8, emphasis is added.). However, this teaching is substantially different from each cryptographic device [in the server

subsystem and not the client] using the private key to verify the retrieved data record, as required by the amended. Iyengar does not teach or suggest the above limitation either.

Accordingly, the combination of Lewis and Iyengar does not teach or suggest the above limitation.

**Third**, regarding the limitation of "each of the plurality of stateless cryptographic devices configured to perform authentication, processing value for the VBI, and generation of indicia data for the plurality of users," as described above, Lewis has one (central) server cryptographic module 14, and many client cryptographic modules 12, one for each client and dedicated to that client. Consequently, each of the client cryptographic modules 12 is not capable of authenticating, processing value for the VBI, and generating indicia data for the plurality of users," rather, at least some of these are the functions of the only (one central) server cryptographic module 14. Iyengar does not teach or suggest the above limitation either.

Accordingly, the combination of Lewis and Iyengar does not teach or suggest the above limitation.

**Fourth**, the limitation of "an available cryptographic device retrieves the data record for the given user . . . from the database," is not disclosed by Lewis's system because, as explained above, Lewis's system has one client cryptographic modules 12 for each client and dedicated to that client. Therefore, a client cryptographic module 12j cannot "retrieve the data record" for a user-k, even though the client cryptographic module 12j may be available. Iyengar does not teach or suggest the above limitation either.

Consequently, the combination of Lewis and Iyengar does not teach or suggest the above limitation.

**Fifth**, regarding the limitation of a "cryptographic device retrieves the data record for the given user directly from the database," Lewis makes it clear that "all sensitive data is stored in a Secure SQL Server Database and protected by SQL Integrated NT security. See FIG. 3. The Secure SQL Server database 305 is considered a part of the server cryptographic 14 module and may only be accessed by the cryptographic module [14]." (Col. 25, lines 55-59, emphasis is added.). Therefore, the client cryptographic modules 12 cannot "retrieve the data record for the

given user directly from the database." Iyengar does not teach or suggest the above limitation either.

Therefore, the combination of Lewis and Iyengar does not teach or suggest the above limitation.

As a result, for at least any of the above five reasons, claim 1 is patentable over the cited references.

Amended independent claim 50 includes, among other limitations, "protecting a data record for each of the plurality of users using a private key, "storing the protected data record for each of the plurality of users in a database remote from the plurality of users," "directly retrieving the data record for a given user from the database," "using the private key to verify the retrieved data record," and "authenticating the given user, processing value for the VBI and generating indicia data for the given user, by any available cryptographic device of the plurality of stateless cryptographic devices." Likewise, Lewis does not teach the above limitation.

**First**, as explained above, the combination of Lewis and Iyengar does not teach or suggest a plurality of stateless cryptographic devices. **Second**, as explained above, the plurality of client cryptographic modules 12 of Lewis cannot authenticate the given user, process value for the VBI and generate indicia data for the given user rather, at least some of these are the functions of the only (one central) server cryptographic module 14. **Third**, as explained above, the combination of Lewis and Iyengar does not teach or suggest "using the private key to verify the retrieved data record." **Fourth**, the combination of Lewis and Iyengar does not disclose "an available cryptographic device retrieves the data record for the given user directly from the database," because, as explained above, Lewis's system has one client cryptographic modules 12 for each client and dedicated to that client.

**Fifth**, client cryptographic modules 12 of Lewis cannot "retrieve the data record for the given user directly from the database," because "database 305 is considered a part of the server cryptographic 14 module and may only be accessed by the cryptographic module [14]." (Id.).


In short, independent claims 1, and 50 define a novel and unobvious invention over the cited references. Dependent claims 5-10, 17, 22, 42, 51, 52, and 55-59 are dependent from

**Appln No. 09/690,796**  
**Amdt date July 18, 2008**  
**Reply to Office action of February 25, 2008**

claims 1 and 50, respectively and therefore include all the limitations of their respective independent claims and additional limitations therein. Accordingly, these claims are also allowable over the cited references, as being dependent from allowable independent claims and for the additional limitations they include therein.

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested.

Respectfully submitted,  
CHRISTIE, PARKER & HALE, LLP

By 

---

Raymond R. Tabandeh  
Reg. No. 43,945  
626/795-9900

RRT/clv

CLV PAS803095.1-\* -07/18/08 3:06 PM